

وكالة الأمن السيبراني الأمريكية تحذر من ثغرتين مستغلتين في نظام Zammad وتدعو للمعالجة الفورية



أضافت وكالة الأمن السيبراني الأمريكية ثغرتين مستغلتين فعلياً في برمجية Zammad إلى قائمة الثغرات المعروفة المستغلة، داعية المؤسسات لمعالجة عيوب تثبيت الجلسات وإدارة الصلاحيات على وجه السرعة.

- إضافة ثغرتين في Zammad (CVE-2026-102489) و CVE-2026-102490 إلى قائمة الثغرات المعروفة المستغلة بسبب الاستغلال النشط
- تتعلق الثغرات بتثبيت الجلسات وإدارة الصلاحيات غير السليمة، وهي نقاط هجوم شائعة للجهات المهددة
- تحث الوكالة جميع المؤسسات وليس الجهات الفيدرالية الأمريكية فقط على تبني إدارة الثغرات القائمة على المخاطر
- الثغرات في الأصول المعرضة للعموم والتي تمنح سيطرة كاملة بعد الاستغلال تتطلب معالجة

- يجب على المؤسسات التحقق من اختراق الأنظمة قبل تطبيق التحديثات الأمنية

أضافت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية ثغرتين توثران على برمجة Zammad إلى قائمة الثغرات المعروفة المستغلة بعد رصد أدلة على استغلالها الفعلي. تؤكد هذه الإضافات المخاطر المستمرة الناجمة عن أنماط الهجوم الشائعة التي تستهدف إدارة الجلسات وضوابط الوصول.

الثغرات وملف المخاطر

الثغرتان هما CVE-2026-102489 المتعلقة بتثبيت الجلسات، و CVE-2026-102490 المتعلقة بإدارة الصلاحيات غير السليمة. تؤثر كلتاها على منصة Zammad من شركة Zammad GmbH. تشير الوكالة إلى أن هذه الأنواع من الثغرات تمثل نقاط هجوم متكررة يستغلها الفاعلون الخبيثون وتشكل مخاطر كبيرة على بيئات المؤسسات، خاصة عند وجودها في الأنظمة المعرضة للعموم.

بموجب التوجيه التشغيلي الملزم 04-26، يجب على الوكالات الفيدرالية الأمريكية إعطاء الأولوية للمعالجة السريعة للثغرات عالية المخاطر، وتحديدًا تلك الموجودة في الأصول المعرضة للعموم والتي تمنح سيطرة كاملة على الأصل بعد الاستغلال الناجح. يحدد التوجيه أيضاً توقعات للوكالات لتحديد ما إذا كانت الجهات المهددة قد اخترقت الأنظمة قبل تطبيق التحديثات.

إرشادات لجميع المؤسسات

رغم أن التوجيه ينطبق فقط على الوكالات المدنية الفيدرالية الأمريكية، تشجع الوكالة جميع المؤسسات عالمياً على تبني ممارسات إدارة الثغرات القائمة على المخاطر وإعطاء الأولوية لمعالجة الثغرات المدرجة في قائمة الثغرات المعروفة المستغلة. تواصل الوكالة تحديث القائمة بناءً على أدلة الاستغلال النشط وتوافر إرشادات المعالجة الواضحة.

يمكن للمؤسسات التي تعلم بثغرات مستغلة غير مدرجة بعد تقديمها عبر نموذج الترشيح الخاص بالوكالة، شريطة توفر معرف CVE وأدلة على الاستغلال وخطوات المعالجة المتاحة.

ما يجب فعله الآن

1. تحديد جميع نسخ برمجة Zammad في بيئتك، خاصة على الأنظمة المعرضة للعموم
2. تطبيق تحديثات المورد لثغرتي CVE-2026-102489 و CVE-2026-102490 فوراً على نشر Zammad المتصل بالإنترنت
3. مراجعة سجلات المصادقة وإدارة الجلسات للبحث عن علامات الاختراق قبل تطبيق التحديثات
4. إجراء اختبارات تصعيد الصلاحيات على الأنظمة المحدثة للتحقق من فعالية المعالجة
5. تحديث إجراءات إدارة الثغرات لإعطاء الأولوية لمدخلات قائمة الثغرات المعروفة المستغلة وفقاً لمتطلبات الضوابط الأساسية للأمن السيبراني وإطار الأمن السيبراني لمؤسسة النقد
6. توثيق الجداول الزمنية للمعالجة وخطوات التحقق لأغراض المراجعة والامتثال